REMARKS

Claims 1, 4-6, 10-13, 18-19, 21-24, 29-33, 36, and 38-67 have been amended. Claims 1-67 remain pending in the application. Reconsideration is respectfully requested in light of the following remarks.

Section 101 Rejection

The Examiner rejected claims 1-67 under 35 U.S.C. § 101 as being directed to non-statutory matter. Specifically, the Examiner submits that the claimed invention is directed toward nothing more than the abstract idea of a mathematical algorithm. Applicants respectfully traverse this rejection. However, to expedite prosecution, the claims have been amended. Specifically, claims 1 and 21 have been amended to recite a method implemented in a device supporting a public-key cryptography application, wherein the device comprises multiple arithmetic circuits that perform various operations of the method, and to recite limitations involving the storage and subsequent use of a generated partial result in a cryptography application. The other independent claims have been similarly amended.

For at least the reasons above, Applicants respectfully request the removal of the rejection of claims 1-67 under 35 U.S.C. § 101.

Section 103 Rejection:

The Examiner rejected claims 1-67 under 35 U.S.C. § 103 as being unpatentable over Gressel et al. (US Patent No. 6,748,410) (hereinafter "Gressel") in view of Striback et al. (US Patent No. 6,181,484). Applicants respectfully traverse this rejection for at least the following reasons.

First, Applicants note that the Examiner inadvertently cited U.S. Patent No. 6,181,484, rather than U.S. Patent No. 7,181,484 (hereinafter "Stribaek").

Regarding claims 1-20, contrary to the Examiner's assertion, Gressel in view of Stribaek fails to disclose all the limitations of these claims. The Examiner cites various passages in Gressel as teaching: feedback of a previous operation into next operation; arithmetic operation or instructions; arithmetic structure; multiplication two values, summing two values utilizing partial (i.e., bit operations, any bit length, high order bits, low order bits) results from previous multiplication; adder; carry-save adder; carry-out; register usage; XOR operations; redundant representation of numbers; acceleration, improvements of arithmetic operations; arithmetic operations utilized to generated cryptography key(s); and processor utilization for key generation. The Examiner submits that Gressel discloses all the limitations of claim 1, in its original form, in these passages, but does not relate the teachings of these passages to any of the specific limitations of claim 1. Instead, the Examiner merely points out the presence of the elements listed above in the system of Gressel.

The Examiner further submits, "Gressel discloses the capability for the multiplication of parameters and circuit, array operations. Gressel does not specifically disclose the usage of Wallace tree multiplication, and extended carry operations. However, Stribaek discloses the usage of Wallace tree columns and multiplications of parameters, and the usage of extended carry operations." The Examiner goes on to cite various passages in Stribaek as teaching Wallace tree; extended carry operations; carry-save adder; and public-key cryptography application **without relating any of these references to any of the specific limitations recited in the claims**.

Applicants assert that the Examiner has failed to address each and every limitation of independent claim 1, and each limitation of dependent claims 2-20 in his remarks. For example, the Examiner's remarks as to the teachings of the cited passages in Gressel do not address all of the specific limitations of claim 1, such as "generating a first partial result of a currently executing arithmetic instruction... the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number." Instead, the Examiner submits that Gressel

teaches, "multiplication two values, summing two values utilizing parallel (i.e., bit operations, any bit length, high order bits, low order bits) results from previous multiplication." **This is clearly not what is recited in claim 1, nor does it teach the limitations of claim 1. Similarly, many of the limitations of claims 2-20 are not mentioned at all in the Examiner's remarks.** Applicants note MPEP 707.07(d), which requires that, in an Examiner's Action, the ground of rejection, should be "fully and clearly stated". **Since the rejection of claims 1-20 has not been fully and clearly stated, Applicants assert that it is improper.**

Further regarding claim 1, Applicants assert that the cited passages do not teach the specific limitations of this claim. For example, the Examiner equates adding a value of "any bit length" and generic references to "high order bits" and "low order bits" to the limitation, "generating a first partial result of a currently executing arithmetic instruction... the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number." Applicants note that the Examiner's cited passage (Gressel, column 2, lines 31-37) states, in its entirety: "Further in accordance with a preferred embodiment of the present invention, the employing step includes multiplying a first integer of any bit length by a second integer of any bit length to obtain a first product, multiplying a third integer of any bit length by a fourth integer of any bit length to obtain a second product, and summing the first and second products with a fifth integer of any bit length to obtain a sum." Applicants first note that this passage describes nothing about "high order bits" or "low order bits" as suggested by the Examiner. **Furthermore, this description of multiplying values of any bit length to obtain products and then adding the products together clearly does not teach the specific limitations of the first partial result recited claim 1, i.e., *the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number.*** In addition, Applicants assert that the cited passages do not teach the additional limitations, "storing the first partial result; and using the stored first partial result in a subsequent computation in the public-key cryptography application," as recited in claim 1.

The Examiner submits that it would have been obvious to one of ordinary skill in the art to modify Gressel as taught by Striback to enable the capability for the usage of Wallace tree multiplication, and that one of ordinary skill in the art would have been motivated to employ the teachings of Striback in order to enable the capability for extended precision in arithmetic calculations due to extensive and increasing use of public key cryptography (citing Striback, column 1, lines 61-67). Applicants note, however, that claim 1 does not recite anything about Wallace tree multiplication, nor has the Examiner relied on anything in Striback to teach the limitations of claim 1. **Applicants assert that Stribaek does not overcome the deficiencies of Gressel in teaching the specific limitations of claim 1.** In Stribaek, microprocessor instructions are provided for manipulating portions of an extended precision accumulator including instructions to move the contents of a portion of the extended accumulator to a general-purpose register and instructions to move the contents of a general-purpose register to a portion of the extended accumulator (see, e.g., Stribaek Abstract, and descriptions of the instructions MFHI, MFLO, MTHI, MTLO, MFLHXU, and MTLHX). Stribaek's system also includes a 32-bit by 16-bit Wallace tree multiplier array that has been modified to support the addition of two 72-bit wide operands ACC1 and ACC2. However, Stribaek (taken alone or in combination with Gressel) does not teach or suggest the specific limitations of Applicants' claimed invention, in which in a partial result is generated through the addition of the specific elements recited in claim 1 in response to a currently executing arithmetic instruction, and a specific feedback operation is performed in response to a previously executed arithmetic instruction.

Applicants respectfully remind the Examiner that to establish a *prima facie* obviousness of a claimed invention, all claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (C.C.P.A. 1974), MPEP 2143.03. The cited art clearly does not teach or suggest all limitations of claim 1, as discussed above.

Applicants assert that numerous ones of dependent claims 2-20 also recite distinctions over the cited art, and that the Examiner has failed to fully and clearly state

his rejection of these claims. Applicants traverse the rejection of these claims for at least the reasons given above in regard to claim 1, from which they depend. However, since the rejections have been shown to be unsupported for independent claim 1, a further discussion of these dependent claims is not necessary at this time. Applicants reserve the right to present additional arguments.

For at least the reasons above, the rejection of claims 1-20 is unsupported by the cited art and removal thereof is respectfully requested.

Independent claims 38 and 66 include limitations similar to those of claim 1, and so the arguments presented above apply with equal force to these claims as well. Dependent claims 39-51 recite limitations similar to those in claims 2-20, and so the arguments presented above apply with equal force to these claims, as well.

Regarding claims 21-37, the Examiner cites the same passages in Gressel and Stribaek and includes the same remarks used to reject claims 1-20 in his rejection of claims 21-37. Therefore, the arguments presented above apply with equal force to these claims, as well. In addition, Applicants note that claim 21 includes limitations different from those in claim 1 and that the Examiner has not specifically addressed these differences in his remarks. Therefore, the rejection of claim 21 is improper. For example, claim 21 includes the limitations "*supplying a third number to the second arithmetic circuit; the second arithmetic circuit generating a first partial result of a currently executing arithmetic instruction in the public-key cryptography application, the first partial result being a representation of the high order bits summed with low order bits of a result of a first number multiplied by a second number and with the third number, the summing being performed during multiplication of the first number and the second number, the summing and at least a portion of the multiplication being performed in the second arithmetic circuit.*" **Applicants assert that the Examiner has cited nothing in the references to teach or suggest these limitations, and that they do not teach these limitations.**

Applicants note that numerous ones of dependent claims 22-37 recite different limitations than those recited in claims 2-20, and that the Examiner did not address these differences in his remarks. Therefore, the rejection of these claims is improper.

For at least the reasons above, the rejection of claims 21-37 is unsupported by the cited art and removal thereof is respectfully requested.

Independent claims 53 and 67 include limitations similar to those of claim 21, and so the arguments presented above apply with equal force to these claims as well. Dependent claims 54-65 recite limitations similar to those in claims 22-37, and so the arguments presented above apply with equal force to these claims, as well.

CONCLUSION

Applicants submit the application is in condition for allowance, and an early notice to that effect is requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/6000-31500/RCK.

Respectfully submitted,

/Robert C. Kowert/
Robert C. Kowert, Reg. #39,255
Attorney for Applicant(s)

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: September 19, 2007